A REMARK ON THE CONJECTURES OF LANG-TROTTER AND SATO-TATE ON AVERAGE

STEPHAN BAIER

ABSTRACT. We obtain new average results on the conjectures of Lang-Trotter and Sato-Tate about elliptic curves.

1. THE CONJECTURES OF SATO-TATE AND LANG-TROTTER

Before we state our results, we first explain briefly the contents of the conjectures of Lang-Trotter and Sato-Tate on elliptic curves.

Let E be an elliptic curve over $\mathbb{Q}$. For any prime number p of good reduction, let $a_p(E)$ be the trace of the Frobenius morphism of $E/\mathbb{F}_p$. Then the number of points on the reduced curve modulo p equals $\#E(\mathbb{F}_p) = p + 1 - a_p(E)$. Furthermore, by Hasse's theorem, $|a_p(E)| \le 2\sqrt{p}$.

For the case that E does not have complex multiplication, Sato and Tate [15] formulated a conjecture on the distribution of angles associated to the numbers $a_p(E)$ which is equivalent to the following assertion on the distribution of the $a_p(E)$'s.

Sato-Tate Conjecture: *Suppose E is an elliptic curve over $\mathbb{Q}$ which does not admit complex multiplication. For any $-1 \le \alpha < \beta \le 1$, and $x \ge 1$, let*

$$\Theta_E(\alpha, \beta; x) := \sum_{\substack{p \le x \\ \alpha \le a_p(E)/(2\sqrt{p}) \le \beta}} \log p.$$

Then

$$\lim_{x \to \infty} \frac{\Theta_E(\alpha, \beta; x)}{x} = \frac{2}{\pi} \int_\alpha^\beta \sqrt{1 - t^2} \, dt.$$

In [4], [10] and [16], L. Clozel, M. Harris, N. Shepherd-Barron and R. Taylor have proved the Sato-Tate conjecture for all elliptic curves E over totally real fields (in particular, over $\mathbb{Q}$) satisfying the mild condition of having multiplicative reduction at some prime.

Lang and Trotter [14] considered the quantity

$$\pi_E^r(x) := \#\{p \le x : a_p(E) = r\},$$

where r is a fixed integer. If $r = 0$ and E has complex multiplication, Deuring [7] showed that

$$(1.1) \qquad \pi_E^0(x) \sim \frac{\pi(x)}{2} \qquad \text{as } x \to \infty.$$

For all other cases, Lang and Trotter [14] conjectured that the following asymptotic estimate holds.

Lang-Trotter Conjecture: *If E has no complex multiplication or $r \neq 0$, we have*

$$\pi_E^r(x) \sim C_{E,r} \pi_{1/2}(x), \qquad \text{as } x \to \infty,$$

where $C_{E,r}$ is some non-negative constant depending on E and r.

Here, as in the sequel,

$$\pi_{1/2}(x) := \int\limits_2^x \frac{\mathrm{d}t}{2\sqrt{t}\log t}.$$

Lang and Trotter [14] used a probabilistic model to give an explicit description of the constant $C_{E,r}$ as an Euler product. The constant can be 0, and the asymptotic estimate is then interpreted to mean that there is only a finite number of primes such that $a_p(E) = r$.

2. Main results

In the sequel, by $E(a, b)$ we denote an elliptic curve given in Weierstrass form

$$y^2 = x^3 + ax + b.$$

As in [1] and [6], we define a constant C_r by

$$C_r := \frac{2}{\pi}\prod_{p|r}\left(1 - \frac{1}{p^2}\right)^{-1}\prod_{p\nmid r}\frac{p(p^2 - p - 1)}{(p-1)(p^2 - 1)}.$$

In particular, if $r = 0$, we have

$$C_0 = \frac{2\zeta(2)}{\pi} = \frac{\pi}{3}.$$

We shall establish the following average estimate of Lang-Trotter-type.

Theorem 1. *Let $\varepsilon > 0$ and $C > 3/2 + \varepsilon$ be given. Fix an integer $r \neq 0$. Then, if*

(2.1) $$A, B > x^\varepsilon \qquad and \qquad x^{3/2+\varepsilon} < AB < x^C,$$

we have, as $x \to \infty$,

(2.2) $$\frac{1}{4AB}\sum_{|a|\leq A}\sum_{|b|\leq B}\pi^r_{E(a,b)}(x) \sim C_r\pi_{1/2}(x).$$

If $r = 0$, then, under the conditions in (2.1), we have, as $x \to \infty$,

(2.3) $$\frac{1}{4AB}\sum_{1\leq|a|\leq A}\sum_{1\leq|b|\leq B}\pi^0_{E(a,b)}(x) \sim \frac{\pi}{3}\pi_{1/2}(x).$$

In (2.3), we have excluded the elliptic curves in the families $E(a, 0)$ and $E(0, b)$ with $a, b \neq 0$ because it turns out that

$$\frac{1}{4AB}\left(\sum_{1\leq|a|\leq A}\pi^0_{E(a,0)}(x) + \sum_{1\leq|b|\leq B}\pi^0_{E(0,b)}(x)\right) \gg \left(\frac{1}{A} + \frac{1}{B}\right)\pi(x)$$

which is much larger than $\frac{\pi}{3}\pi_{1/2}(x)$ if A, B are small compared to $\sqrt{x}$. This is due to the fact that the curves in the said families have complex multiplication in which case we have Deuring's result (1.1).

All other curves with complex multiplication are of the form $E_{(\alpha_i t^2, \beta_i t^3)}$, where $t \in \mathbb{Z}/\{0\}$, and (α_i, β_i) is in an explicit set of eleven pairs of integers (see [8], page 3, for example). Hence, if $AB > x^{3/2+\varepsilon}$, their contribution to (2.3) is

$$\ll \frac{\min\{A^{1/2}, B^{1/3}\}}{AB}\pi(x) \ll \frac{x}{\sqrt{AB}} \ll x^{1/4}$$

which is negligible compared to the main term.

In [1], we proved Theorem 1 under the conditions

$$A, B > x^{1/2+\varepsilon} \qquad and \qquad AB > x^{3/2+\varepsilon}$$

in place of (2.1). Hence, unlike the corresponding Theorem 2 in [1], the above Theorem 1 applies to situations when A and B are very small compared to $x^{1/2}$. Our additional condition $AB < x^C$ in Theorem 1 is not

a real constraint since we are mainly interested in averages for small A's and B's, and it is likely that this condition can be removed by a refined treatment of a certain error term in section 3.

We further note that the above-mentioned Theorem 2 in [1] in turn was a generalization of an average result by E. Fouvry and M.R. Murty [8] on $\pi^0_{E(a,b)}(x)$ and an improvement of a result of C. David and F. Pappalardi [6] who showed the asymptotic formula (2.2) under the stronger condition $A, B > x^{1+\varepsilon}$.

Moreover, we shall prove the following average result on the Sato-Tate conjecture.

Theorem 2. *Let $\varepsilon, c > 0$ and $C > 3/2 + 2\varepsilon$ be given. Further, let $x \geq 1$ and $0 < \alpha < \beta \leq 1$. Set*

$$(2.4) \qquad F(\alpha, \beta) := \frac{2}{\pi} \int_\alpha^\beta \sqrt{1 - t^2} \, \mathrm{d}t \qquad and \qquad \gamma := \beta - \alpha.$$

Assume that $x^{\varepsilon - 5/12} \leq \gamma/\beta \leq x^{-\varepsilon}$ and $F(\alpha, \beta) \geq x^{-1/2+\varepsilon}$. Then, if

$$(2.5) \qquad A, B > x^\varepsilon \qquad and \qquad x^{1+\varepsilon}/F(\alpha, \beta) < AB < x^C,$$

we have

$$(2.6) \qquad \frac{1}{4AB} \sum_{1 \leq |a| \leq A} \sum_{1 \leq |b| \leq B} \Theta_{E(a,b)}(\alpha, \beta; x) = xF(\alpha, \beta)\left(1 + O\left(\frac{1}{\log^c x}\right)\right),$$

where the implied O-constant depends only on ε, c and C.

To avoid technical complications, we have excluded the cases when $ab = 0$. This makes sense because, as mentioned above, all elliptic curves $E(a, 0)$ and $E(0, b)$ $(a, b \neq 0)$ have complex multiplication, and the Sato-Tate conjecture is exclusively formulated for curves *without* complex multiplication (if E has complex multiplication, the distribution of the $a_p(E)$'s is different from the Sato-Tate distribution).

We recall that the number of all remaining curves with complex multiplication is $O(\min\{A^{1/2}, B^{1/3}\})$. Hence, if $AB > x^{1+\varepsilon}/F(\alpha, \beta)$, their contribution to (2.6) is, by a trivial estimation,

$$\ll \frac{\min\{A^{1/2}, B^{1/3}\}}{AB} x \ll \frac{x}{\sqrt{AB}} \ll x^{1/2}$$

which is majorized by the error term $xF(\alpha, \beta)/\log^c x$ since we assume that $F(\alpha, \beta) \geq x^{-1/2+\varepsilon}$.

In [2], L. Zhao and I proved Theorem 2 (with the cases when $ab = 0$ included) under the conditions

$$A, B > x^{1/2+\varepsilon} \qquad and \qquad AB > x^{1+\varepsilon}/F(\alpha, \beta)$$

in place of (2.5). Again, Theorem 2 in the present paper allows much more flexibility in the choice of A and B, and the condition $AB < x^C$ therein is not a real constraint.

From Theorem 2, we derive the following corollary on the Sato-Tate conjecture on average for *fixed* α and β.

Corollary 1. *Let $\varepsilon, c > 0$ and $C > 1 + \varepsilon$ be given, and let α, β be fixed real numbers with $0 < \alpha < \beta < 1$. Define $F(\alpha, \beta)$ as in Theorem 2. Then, if*

$$(2.7) \qquad A, B > x^\varepsilon \qquad and \qquad x^{1+\varepsilon} < AB < x^C,$$

we have, as $x \to \infty$,

$$(2.8) \qquad \frac{1}{4AB} \sum_{1 \leq |a| \leq A} \sum_{1 \leq |b| \leq B} \Theta_{E(a,b)}(\alpha, \beta; x) = xF(\alpha, \beta)\left(1 + O\left(\frac{1}{\log^c x}\right)\right),$$

where the implied O-constant depends only on α, β, ε, c and C.

Proof. If $0 < \alpha < \beta < 1$ and x is sufficiently large, then it is possible to split the interval $[\alpha, \beta]$ into a finite number of subintervals $[\alpha', \beta']$ satisfying $x^{-2\varepsilon/3} \leq (\beta' - \alpha')/\beta' = \gamma'/\beta' \leq x^{-\varepsilon/3}$ and $F(\alpha', \beta') \geq x^{-2\varepsilon/3}$. Now applying Theorem 2 with ε replaced by $\varepsilon/3$ to each of these subintervals, and summing up all contributions, we obtain the desired asymptotic estimate (2.8) under the conditions in (2.7). $\qquad\square$

We note that Theorem 14 in the recent work [3] of W. Banks and I.E. Shparlinski implies the asymptotic estimate (2.8) as well (the contributions of a, b with $ab = 0$ is negligible), but they require the conditions

$$x^\varepsilon < A, B \leq x^{1-\varepsilon} \quad \text{and} \quad AB > x^{1+\varepsilon} \sqrt{\min\{A, B\}}$$

which are stronger than our conditions in (2.7).

On the other hand, their error term estimate is *uniform* with respect to α and β, unlike that in our Corollary 1, and their estimate is sharper than ours by a factor of $x^{-\delta}$. Moreover, their result is valid for all α, β with $-1 \leq \alpha < \beta \leq 1$ (in fact, they consider angles corresponding to α and β, which lie in the interval $[0, \pi]$). Our method certainly works for α, β with $-1 < \alpha < \beta < 0$ as well, but so far it doesn't cover intervals $[\alpha, \beta]$ containing -1, 0 or 1.

We note that the work of L. Clozel, M. Harris, N. Shepherd-Barron and R. Taylor in [4], [10] and [16] on the Sato-Tate conjecture for individual elliptic curves does not imply any of the above average results due to the lack of uniformity of the error term with respect to a and b, and due to the lack of sufficiently strong zero density estimates for symmetric power L-functions. (Such zero density estimates would be required to establish a version of the Sato-Tate conjecture on individual elliptic curves for *small* intervals $[\alpha, \beta]$.)

We achieve our improvements by employing an almost-all result on character sums by Banks and Shparlinski which played an important rule in their paper [3] too and is a consequence of a more general result by Garaev [9]. This result turns out to be more useful in the estimation of certain error terms than the bound of Polya-Vinogradov, which we used in [1] and [2] at corresponding places, since it applies to very short character sums.

3. Proof of Theorem 1

In the following, let $r \neq 0$. We first estimate the contribution of all elliptic curves in the families $E(a, 0)$ and $E(0, b)$ $(a, b \neq 0)$. We again note that these curves have complex multiplication. Further, if E is an elliptic curve with complex multiplication, then, with an absolute $\ll$-constant not depending on E or r, we have the bound

$$\pi_E^r(x) \ll x^{1/2}.$$

This is due to the fact that if E has complex multiplication and $r \neq 0$, then the primes p satisfying $a_p(E) = r$ are of the form $p = f_{E,r}(n)/4$, where n is an integer and $f_{E,r}$ is a certain quadratic polynomial with integer coefficients (see the equation and inequality before Theorem 9 in [5]). It follows that if $r \neq 0$, then

$$(3.1) \qquad \frac{1}{4AB} \left(\sum_{1 \leq |a| \leq A} \pi_{E(a,0)}^r(x) + \sum_{1 \leq |b| \leq B} \pi_{E(0,b)}^r(x) \right) \ll \left(\frac{1}{A} + \frac{1}{B} \right) x^{1/2} \ll x^{1/2-\varepsilon}.$$

It remains to estimate the sum

$$\sum_{1 \leq |a| \leq A} \sum_{1 \leq |b| \leq B} \pi_{E(a,b)}^r(x),$$

where we now admit all integers r (including $r = 0$). Here we follow our method in [1], with the alteration that we use a result due to Banks, Shparlinski and Garaev instead of the Polya-Vinogradov estimate to bound a certain error term. We shall be brief at all places where we don't alter the method in [1].

Similarly as in equation (2.2) in [1], the quantity in question can be written in the form

$$(3.2) \qquad \sum_{1 \leq |a| \leq A} \sum_{1 \leq |b| \leq B} \pi_{E(a,b)}^r(x) = \sum_{B(r) < p \leq x} \sharp\{1 \leq |a| \leq A, \ 1 \leq |b| \leq B \ : \ a_p(E(a,b)) = r\},$$

where $B(r) = \max\{3, r, r^2/4\}$. In [1], we first estimated the contribution of a's and b's with $p | ab$ by

$$(3.3) \qquad \ll \frac{AB}{p} + A + B,$$

which turned out to be a small enough error term. We then evaluated the remaining term

$$\sharp\{|a| \leq A, \ |b| \leq B \ : \ p \nmid ab, \ a_p(E(a,b)) = r\}.$$

In the present note, the bound (3.3) is not sufficient due to the fact that we admit A's and B's that are much smaller than in [1]. In the following, we establish a refined estimate for the contribution in question. We observe that

$$(3.4) \qquad \sum_{B(r)<p\leq x} \sharp\{1 \leq |a| \leq A, 1 \leq |b| \leq B \ : \ p|ab, \ a_p(E(a,b))=r\}$$

$$\leq \quad 4 \sum_{1\leq a\leq A} \sum_{1\leq b\leq B} \sum_{p|ab} 1$$

$$\leq \quad 4 \sum_{n\leq AB} \tau(n)^2$$

$$\ll \quad (AB)^{1+\varepsilon_0}$$

for every fixed $\varepsilon_0 > 0$, where $\tau(n)$ is the number of divisors of n. By (3.4) and our condition $AB < x^C$ in Theorem 2, the above contribution is indeed negligible if $C < 1/(2\varepsilon_0)$.

The remaining term is

$$\sum_{B(r)<p\leq x} \sharp\{|a| \leq A, \ |b| \leq B \ : \ p\nmid ab, \ a_p(E(a,b))=r\},$$

which we shall evaluate in the following. By Lemma 1 in [1] (see also Lemma 1 in [2]) due to Deuring, the total number of $\mathbb{F}_p$-isomorphism classes of elliptic curves $E(c,d)$ over $\mathbb{F}_p$ with $p+1-r$ points equals the Kronecker class number $H(r^2-4p)$. Let $I_{r,p}$ be the number of $\mathbb{F}_p$-isomorphism classes of elliptic curves $E(c,d)$ over $\mathbb{F}_p$ with $p+1-r$ points such that $c,d \neq 0$. Hence,

$$(3.5) \qquad I_{r,p} \leq H(r^2-4p).$$

Let $(u_{p,j}, v_{p,j})$, $j = 1,...,I_{r,p}$ be pairs of integers such that the curves $E(\overline{u_{p,j}}, \overline{v_{p,j}})$ form a system of representatives of these isomorphism classes, where $\overline{n}$ denotes the reduction of an integer n modulo p. Let $(\cdot/p)_4$ be the biquadratic residue symbol. Then, as observed in section 4 in [1], if $p \equiv 1 \bmod 4$, we have

$$(3.6) \qquad \sharp\{|a| \leq A, \ |b| \leq B \ : \ p\nmid ab, \ a_p(E(a,b))=r\}$$

$$= \quad \frac{1}{4\varphi(p)} \sum_{k=1}^{4} \sum_{\chi \bmod p} \sum_{j=1}^{I_{r,p}} \left(\frac{u_{p,j}}{p}\right)_4^{-k} \overline{\chi}^3(u_{p,j})\chi^2(v_{p,j}) \sum_{|a|\leq A} \left(\frac{a}{p}\right)_4^{k} \chi^3(a) \sum_{|b|\leq B} \overline{\chi}^2(b)$$

$$= \quad M(p) + E_1(p) + E_2(p),$$

where

$M(p) = $ contribution of k, χ with $(\cdot/p)_4^k \chi^3 = \chi_0, \ \chi^2 = \chi_0$;

$E_1(p) = $ contribution of k, χ with $(\cdot/p)_4^k \chi^3 \neq \chi_0, \ \chi^2 = \chi_0$ or $(\cdot/p)_4^k \chi^3 = \chi_0, \ \chi^2 \neq \chi_0$;

$E_2(p) = $ contribution of k, χ with $(\cdot/p)_4^k \chi^3 \neq \chi_0, \ \chi^2 \neq \chi_0$.

As noted in [1], in the case $p \equiv 3 \bmod 4$, a similar representation of the term

$$\sharp\{|a| \leq A, \ |b| \leq B \ : \ p\nmid ab, \ a_p(E(a,b))=r\}$$

as a character sum is possible, and this expression can be treated in a similar way as the above expression in the case $p \equiv 1 \bmod 4$. Therefore, as in [1], we can confine ourselves to primes p with $p \equiv 1 \bmod 4$.

In [1] we used results in [6] to treat the the main term $M(p)$. The error term $E_1(p)$ was estimated by using the Polya-Vinogradov inequality, and the error term $E_2(p)$ was handled by the Cauchy-Schwarz inequality and some mean value estimates for character sums. Our estimate for $E_1(p)$ gave rise to the condition $A, B \geq x^{1/2+\varepsilon}$ in Theorem 2 in [1], and our estimate for $E_2(p)$ gave rise to the condition $AB \geq x^{3/2+\varepsilon}$ in the same theorem.

In the following, we want to refine the estimation of

$$\sum_{\substack{B(r)<p\leq x \\ p\equiv 1 \bmod 4}} |E_1(p)|$$

by using the following variant of an almost-all result on character sums of Banks and Shparlinski [3] which is contained in a more general result, Theorem 10 in [9], of Garaev.

Lemma 1. *Fix $\varepsilon > 0$ and $\eta > 0$. If $x > 0$ is sufficiently large, then for all $M \geq x^{\varepsilon}$, all primes with at most $x^{3/4+4\eta+o(1)}$ exceptions, and all non-principal multiplicative characters χ modulo p, we have*

$$\left| \sum_{|n| \leq M} \chi(n) \right| \leq M^{1-\eta},$$

where the function implied by $o(1)$ depends only on ε and η.

Proof. This is Lemma 3 in [3], except that there the above sum is replaced by

$$\sum_{n=1}^{M} \chi(n).$$

But

$$\sum_{|n| \leq M} \chi(n) = (1 + \chi(-1)) \sum_{n=1}^{M} \chi(n)$$

and hence, the result follows. $\square$

We also need the following bound for $I_{r,p}$.

Lemma 2. *If $|r| < 2\sqrt{p}$, then*

$$I_{r,p} \leq H(r^2 - 4p) \ll p^{1/2} \log^2 p.$$

Proof. The inequality $I_{r,p} \leq H(r^2 - 4p)$ was stated in (3.5). By Lemma 3 in [2], for the Kronecker class number $H(r^2 - 4p)$ we have the formula

$$H(r^2 - 4p) = \frac{1}{\pi} \sum_{\substack{f,d \\ r^2 - 4p = df^2 \\ d \equiv 0,1 \mod 4}} \sqrt{|d|} L(1, \chi_d),$$

where χ_d is a certain real character with conductor $\ll d$ (the above formula follows from a relation between the Kronecker and Dirichlet class numbers, and the Dirichlet class number formula). Now using the well-known bound

$$L(1, \chi_d) \ll \log d,$$

the desired result follows by a quick computation. $\square$

As noted in [1], for each k the number of characters χ modulo p satisfying $(\cdot/p)_4^k \chi^3 \neq \chi_0$, $\chi^2 = \chi_0$ or $(\cdot/p)_4^k \chi^3 = \chi_0$, $\chi^2 \neq \chi_0$ is bounded. Therefore, Lemma 2 implies the bound

$$(3.7) \qquad |E_1(p)| \ll \frac{\log^2 p}{p^{1/2}} \left(A \max_{\substack{\chi \bmod p \\ \chi \neq \chi_0}} \left| \sum_{|b| \leq B} \chi(b) \right| + B \max_{\substack{\chi \bmod p \\ \chi \neq \chi_0}} \left| \sum_{|a| \leq A} \chi(a) \right| \right).$$

From (3.7) and Lemma 1 with $\eta = 1/20$, we now obtain

$$(3.8) \qquad \sum_{\substack{B(r) < p \leq x \\ p \equiv 1 \bmod 4}} |E_1(p)| \ll x^{1/2} (\log x)^2 A B^{19/20} + x^{1/2} (\log x)^2 A^{19/20} B + x^{9/20+\varepsilon} AB.$$

Similarly, one can prove that

$$(3.9) \qquad \sum_{\substack{B(r) < p \leq x \\ p \equiv 3 \bmod 4}} |E_1(p)| \ll x^{1/2} (\log x)^2 A B^{19/20} + x^{1/2} (\log x)^2 A^{19/20} B + x^{9/20+\varepsilon} AB.$$

Moreover, from the first equation after (4.3) in [1], Lemma 3 in [1], and Lemma 2 above, we deduce that

$$(3.10) \qquad \sum_{B(r) < p \leq x} M(p) = 4 C_r \pi_{1/2}(x) AB + O\left(\frac{AB\sqrt{x}}{\log^c x} \right)$$

for any given $c > 0$, and from the first inequality after (4.4) in [1] and Lemma 2 above, we deduce that

$$(3.11) \qquad \sum_{B(r) < p \leq x} |E_2(p)| \ll x^{5/4}(\log x)^4 (AB)^{1/2}.$$

Now, combining (3.2), (3.4), (3.6), (3.8), (3.9), (3.10) and (3.11), we obtain the estimate

$$(3.12) \quad \frac{1}{4AB} \sum_{1 \leq |a| \leq A} \sum_{1 \leq |b| \leq B} \pi^r_{E(a,b)}(x)$$

$$= C_r \pi_{1/2}(x) + O\left((AB)^{\varepsilon_0 - 1} + x^{1/2}(\log x)^2 \left(\frac{1}{A^{1/20}} + \frac{1}{B^{1/20}} + \frac{1}{x^{1/20 - \varepsilon}} \right) + \frac{x^{5/4} \log^4 x}{\sqrt{AB}} + \frac{\sqrt{x}}{\log^c x} \right).$$

From (3.1) and (3.12), we deduce that the desired asymptotic estimates (2.2) and (2.3) hold under the conditions in (2.1). This completes the proof of Theorem 1.

4. PROOF OF THEOREM 2

We follow our method in [2], with the alteration that we again use Lemma 1 instead of the Polya-Vinogradov estimate to bound a certain error term. Since we proceed similarly as in the previous section, we shall be very brief. Similarly as in [2] and in the previous section, we first write the quantity

$$\sum_{1 \leq |a| \leq A} \sum_{1 \leq |b| \leq B} \Theta_{E(a,b)}(\alpha, \beta; x)$$

in question as a character sum $\mathcal{X}$ plus some error term which can be bounded in a similar way as in (3.4) and is negligible under the condition $AB < x^C$ with $C > 3/2 + 2\varepsilon$ being arbitrarily given. We then split our character sum $\mathcal{X}$ into a main term of the form

$$\mathcal{M} = \sum_{p \leq x} M(p)$$

and two error terms $\mathcal{E}_1, \mathcal{E}_2$ of the form

$$\mathcal{E}_i = \sum_{p \leq x} E_i(p).$$

We don't change our treatments of the main term and the second error term in [2] at all. To bound these terms, we required the conditions $F(\alpha, \beta) \geq x^{-1/2 + \varepsilon}$, $x^{\varepsilon - 5/12} \leq \gamma/\beta \leq x^{-\varepsilon}$ and $AB > x^{1+\varepsilon}/F(\alpha, \beta)$ in [2]. The treatment of the first error term in [2] led to the additional condition $A, B > x^{1/2 + \varepsilon}$ which we aim to replace by $A, B > x^\varepsilon$. To this end, we need to estimate this error term $\mathcal{E}_1$ by a different technique.

For the proof of Theorem 2 it now suffices to establish that

$$(4.1) \qquad \frac{1}{4AB} |\mathcal{E}_1| \ll F(\alpha, \beta) \frac{x}{\log^c x}$$

holds for every fixed $c > 0$ if $A, B > x^\varepsilon$. By the considerations in [2], if $p \equiv 1 \bmod 4$, then $E_1(p)$ is of the form

$$(4.2) \qquad E_1(p) = \frac{1}{4\varphi(p)} \sum_{k=1}^{4} {\sum_{\chi \bmod p}}' \sum_{j=1}^{I_p} \left(\frac{u_{p,j}}{p} \right)_4^{-k} \overline{\chi}^3(u_{p,j}) \chi^2(v_{p,j}) \sum_{|a| \leq A} \left(\frac{a}{p} \right)_4^k \chi^3(a) \sum_{|b| \leq B} \overline{\chi}^2(b),$$

where the sum ${\sum_{\chi \bmod p}}'$ is taken over all characters such that $(\cdot/p)_4^k \chi^3 \neq \chi_0$, $\chi^2 = \chi_0$ or $(\cdot/p)_4^k \chi^3 = \chi_0$, $\chi^2 \neq \chi_0$, the number I_p satisfies the bound

$$(4.3) \qquad I_p \leq \sum_{2\sqrt{p}\alpha \leq r \leq 2\sqrt{p}\beta} H(r^2 - 4p) =: H_p,$$

and $u_{p,j}, v_{p,j}$ are certain integers. By (5.4) in [2] and our condition $F(\alpha, \beta) \geq x^{-1/2 + \varepsilon}$, we have the bound

$$(4.4) \qquad H_p \ll x^{1+\varepsilon_1} F(\alpha, \beta)$$

for any fixed $\varepsilon_1 > 0$, the implied $\ll$-constant depending only on ε_1. Using (4.2), (4.3), (4.4) and the fact that the number of summands of the sum $\sum\limits_{\chi \bmod p}'$ is bounded, we deduce that

$$(4.5) \qquad |E_1(p)| \ll \frac{x^{1+\varepsilon_1} F(\alpha,\beta)}{p} \left(A \max_{\substack{\chi \bmod p \\ \chi \neq \chi_0}} \left| \sum_{|b| \leq B} \chi(b) \right| + B \max_{\substack{\chi \bmod p \\ \chi \neq \chi_0}} \left| \sum_{|a| \leq A} \chi(a) \right| \right).$$

Now using (4.5) and Lemma 1 with $\eta = 1/20$, we obtain

$$(4.6) \qquad \sum_{\substack{p \leq x \\ p \equiv 1 \bmod 4}} |E_1(p)| \ll x^{1+2\varepsilon_1} F(\alpha,\beta) A B^{19/20} + x^{1+2\varepsilon_1} F(\alpha,\beta) A^{19/20} B + x^{19/20+\varepsilon} F(\alpha,\beta) A B.$$

If $p \equiv 3 \bmod 4$, then the term $E_1(p)$ can be written as a character sum similar to (4.2) and be estimated by the same method. This leads to the same bound for $\sum\limits_{\substack{p \leq x \\ p \equiv 3 \bmod 4}} |E_1(p)|$ as (4.6). Therefore, we obtain

$$|\mathcal{E}_1| \leq \sum_{p \leq x} |E_1(p)| \ll x^{1+2\varepsilon_1} F(\alpha,\beta) A B^{19/20} + x^{1+2\varepsilon_1} F(\alpha,\beta) A^{19/20} B + x^{19/20+\varepsilon} F(\alpha,\beta) A B$$

which is

$$\ll \frac{x F(\alpha,\beta)}{\log^c x}$$

for every fixed $c > 0$ if $A, B \geq x^\varepsilon$, as desired. This completes the proof of Theorem 2.

References

[1] S. Baier, *The Lang-Trotter conjecture on average*, to appear in J. Ramanujan Math. Soc., arXiv:math.NT/0609095.

[2] S. Baier, L. Zhao, *The Sato-Tate Conjecture on Average for Small Angles*, to appear in Trans. Am. Math. Soc., arXiv:math.NT/0608318.

[3] W. D. Banks, I. E. Shparlinski, *Sato-Tate, cyclicity, and divisibility statistics on average for elliptic curves of small height*, preprint, ArXiv:math.NT/0609144.

[4] L. Clozel, M. Harris, and R. Taylor, *Automorphy for some l-adic lifts of automorphic mod l Galois representations*, preprint, available at www.math.harvard.edu/~rtaylor.

[5] A.C. Cojocaru, *Questions about the reductions modulo primes of an elliptic curve*, Proceedings of the 7-th conference of the Canadian Number Theory Association (Montreal, 2002), ed. E. Goren and H. Kisilevsky, CRM Proceedings and Lecture Notes, Vol. 36 (2004) 61-79.

[6] C. David, F. Pappalardi, *Average Frobenius Distributions of Elliptic Curves*, Int. Math. Res. Not. (1999) 165-183.

[7] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. 14 (1941) 197-272.

[8] E. Fouvry, M.R. Murty, *On the distribution of supersingular primes*, Canad. J. Math. 48 (1996) 81-104.

[9] M.Z. Garaev, *Character sums in short intervals and the multiplication table modulo a large prime*, Monat. Math. 148 (2006) 127-138.

[10] M.Harris, N. Shepherd-Barron and R. Taylor, *Ihara's lemma and potential automorphy*, preprint, available at www.math.harvard.edu/~rtaylor.

[11] H. Iwaniec, E. Kowalski, *Analytic Number Theory*, American Mathematical Society Colloquium Publications, American Mathematical Society, vol. 53.

[12] K. James, G. Yu, *Average Frobenius Distribution of Elliptic Curves*, Acta Arith. 124 (2006), 79–100.

[13] N. Jones, *The constants in the Lang-Trotter conjecture*, preprint (2006).

[14] S. Lang, H. Trotter, *Frobenius Distributions in GL_2 extensions*, Lecture Notes in Math. 504 (1976) Springer-Verlag, Berlin.

[15] J.T. Tate, *Algebraic cycles and poles of zeta functions*, Arithmetical algebraic Geom., Harper and Row, New York, 1965.

[16] R. Taylor, *Automorphy for some l-adic lifts of automorphic mod l representations II*, preprint, available at www.math.harvard.edu/~rtaylor.

Stephan Baier

School of Engineering and Science, Jacobs University Bremen

P. O. Box 750561, Bremen 28725, Germany

Email: `s.baier@jacobs-university.de`